

**BURSOR & FISHER, P.A.**

Brittany S. Scott (State Bar No. 327132)  
1990 North California Blvd., Suite 940  
Walnut Creek, CA 94596  
Telephone: (925) 300-4455  
Facsimile: (925) 407-2700  
E-mail: bscott@bursor.com

**BURSOR & FISHER, P.A.**

Philip L. Fraietta (State Bar No. 354768)  
1330 Avenue of the Americas, 32nd Floor  
New York, NY 10019  
Telephone: (646)-837-7150  
Facsimile: (212) 989-9163  
Email: pfraietta@bursor.com

*Attorneys for Plaintiff*

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF CALIFORNIA**

TIM HARVEY, individually and on behalf of all  
others similarly situated,

Plaintiff,

v.

INSTANT URGENT CARE and PRACTICE  
CROWN INC.,

Defendants.

Case No.

**CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

Plaintiff Tim Harvey (“Plaintiff”) brings this class action complaint on behalf of himself and all others similarly situated against Instant Urgent Care and Practice Crown Inc. (collectively, “Defendants”). Plaintiff brings this action based upon personal knowledge of the facts pertaining to himself, and on information and belief as to all other matters, by and through the investigation of undersigned counsel.

### **NATURE OF THE ACTION**

1. This is a class action lawsuit brought on behalf of all California residents who have accessed and used the website owned, operated and controlled by Defendant Instant Urgent Care, <https://instantuc.com/> (the “Website”). This class action lawsuit is also brought on behalf of all U.S. residents who scheduled their medical appointments through the online booking platform hosted by Defendant Practice Crown Inc. (the “Online Booking Platform”).

2. Unbeknownst to consumers, Defendant Instant Urgent Care assists Defendant Practice Crown Inc. in obtaining its patients' protected health information (“PHI”) and personally identifiable information (“PII”) when they schedule appointments on the Website through the Online Booking Platform.

3. Defendants also aid, employ, agree, and conspire with Meta Platforms, Inc., formerly known as Facebook, Inc. (“Facebook”) to intercept communications sent and received by Plaintiff and Class Members, including communications containing PHI and PII.

4. Plaintiff brings this action for legal and equitable remedies resulting from these illegal actions.

### **PARTIES**

#### ***Plaintiff***

5. Plaintiff Tim Harvey is an adult citizen of the state of California and is domiciled in McClellan, California.

6. Plaintiff accessed the Website in or around May 2024 to schedule an urgent care appointment at Defendant Instant Urgent Care’s Natomas, Sacramento location. When making the appointment on the Website through the Online Booking Platform, Plaintiff disclosed that the reason for the appointment was “sore throat and persistent cough.” Plaintiff also disclosed several

1 other pieces of personal information, including his name, sex, date of birth, home address, email  
2 address, marital status, and social security number.

3 7. Because of Defendants' actions as alleged herein, Plaintiff's use of the Website and  
4 Online Booking Platform has led to the unlawful interception of his PHI and PII. Specifically, as a  
5 result of Defendants' unlawful conduct as alleged herein, Plaintiff's medical symptoms, name, sex,  
6 date of birth, home address, email address, marital status, and social security number were  
7 disclosed to Defendant Practice Crown Inc. without Plaintiff's knowledge or consent. Similarly,  
8 Defendants assisted Facebook with intercepting information about the medical appointment  
9 Plaintiff scheduled on the Website through the Booking Platform, including a description of the  
10 appointment, and the location of the appointment. As a result of Defendants' unlawful conduct,  
11 Plaintiff began receiving digital advertisements related to this medical appointment.

12 8. Plaintiff has an active Facebook account which he has maintained during all  
13 relevant times prior to and after scheduling a medical appointment on the Website through the  
14 Online Booking Platform. During that time, Plaintiff routinely logged onto his Facebook account  
15 on the same web browser he has used to access the Website.

16 9. Pursuant to the systematic process described herein, Defendant Instant Urgent Care  
17 disclosed Plaintiff's PHI and PII to Defendant Practice Crown Inc. Defendants also assisted  
18 Facebook with intercepting Plaintiff's communications, including those that contained PHI, PII,  
19 and related confidential information. Defendants assisted these interceptions without Plaintiff's  
20 knowledge, consent, or express written authorization.

21 10. By failing to receive the requisite consent, Defendants breached its duties of  
22 confidentiality and unlawfully disclosed Plaintiff's PII and PHI.

23 ***Defendants***

24 11. Instant Urgent Care is incorporated in the State of California and has its principal  
25 place of business in San Jose, California. Instant Urgent Care is "a healthcare facility that provides  
26 immediate medical help for non-life-threatening conditions."<sup>1</sup> Instant Urgent Care also offers  
27

28 <sup>1</sup> INSTANT URGENT CARE, <https://instantuc.com/about-us/>.

1 primary care medical services, including sick visits, flu shots, STD testing, and immigration  
2 physicals. Patients can book appointments through its Website, <https://instantuc.com/>. Instant  
3 Urgent Care owns, operates, and controls the Website. Defendant Instant Urgent Care contracts  
4 with Defendant Practice Crown Inc. for services related to digital marketing and online  
5 appointment booking.

6 12. Practice Crown Inc. is incorporated in the State of Delaware and has its principal  
7 place of business in Palo Alto, California. Practice Crown Inc. partners with medical facilities,  
8 including Defendant Instant Urgent Care, to provide “cutting-edge website development, []  
9 targeted digital marketing, and seamless online appointment booking[.]”<sup>2</sup> Consumers who book an  
10 appointment on the Website are directed to the Online Booking Platform hosted by Practice Crown  
11 to finalize the appointment scheduling process. However, Defendant Practice Crown Inc.  
12 constructs its platforms to mimic the webpages of its clients. Therefore, while a consumer may  
13 believe they are interacting with and sharing their PHI and PII with their health care provider,  
14 Defendant Instant Urgent Care, they are actually sharing this confidential information with an  
15 unknown third party, Practice Crown Inc.

### 16 **JURISDICTION AND VENUE**

17 13. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(A)  
18 because this case is a class action where the aggregate claims of all members of the proposed class  
19 are in excess of \$5,000,000, exclusive of interest and costs, and at least one member of the  
20 proposed class is a citizen of a state different from at least one Defendant.

21 14. The Court has general personal jurisdiction over Defendant Instant Urgent Care  
22 because Instant Urgent Care resides in and does business in the State of California, with its  
23 principal place of business in San Jose, California. The Court has general personal jurisdiction  
24 over Defendant Practice Crown Inc. because Practice Crown Inc. resides in and does business in  
25 the State of California, with its principal place of business in Palo Alto, California.

26  
27  
28 <sup>2</sup> PRACTICE CROWN INC., <https://practicecrown.com/about>.

15. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b)(1) because Defendants reside in this District.

### **FACTUAL ALLEGATIONS**

#### **A. Background of the California Information Privacy Act**

16. The CIPA, Cal. Penal Code § 630, *et seq.*, prohibits aiding or permitting another person to willfully—and without the consent of all parties to a communication—read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from or received at any place within California.

17. To establish liability under Cal. Penal Code § 631(a), a plaintiff need only establish that the defendant, “by means of any machine, instrument, contrivance, or in any other manner,” does any of the following:

Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,  
Or

Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,  
Or

Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,  
Or

Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

18. Section 631(a)’s applicability is not limited to phone lines, but also applies to “new technologies” such as computers, the internet, and email. *See Matera v. Google Inc.*, 2016 WL 8200619, at \*21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to “new technologies” and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at \*5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs “electronic

communications”); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook’s collection of consumers’ internet browsing history).

19. Under Cal. Penal Code § 637.2, Plaintiff and Class Members may seek injunctive relief and statutory damages of \$5,000 per violation.

**B. Background of the California Confidentiality of Medical Information Act**

20. Pursuant to the California Confidentiality of Medical Information Act (“CMIA”), “A provider of health care ... shall not disclose medical information regarding a patient of the provider of health care ... without first obtaining an authorization, except as provided in subdivision (b) or (c).” Cal. Civ. Code § 56.10(a).<sup>3</sup> “An authorization for the release of medical information ... shall be valid if it:

(a) Is handwritten by the person who signs it or is in a typeface no smaller than 14-point type.

(b) Is clearly separate from any other language present on the same page and is executed by a signature which serves no other purpose than to execute the authorization.

(c) Is signed and dated ...

(d) States the specific uses and limitations on the types of medical information to be disclosed.

(e) States the name or functions of the provider of health care, health care service plan, pharmaceutical company, or contractor that may disclose the medical information.

(f) States the name or functions of the persons or entities authorized to receive the medical information.

(g) States the specific uses and limitations on the use of the medical information by the persons or entities authorized to receive the medical information.

<sup>3</sup> Subdivisions (b) and (c) are not relevant to this case but permit the disclosure of medical information in situations where a government investigation or lawsuit is taking place. For example, Instant Urgent Care could bypass the authorization requirement if patient medical information was requested pursuant to a lawful court order or by a party to a proceeding before a court or administrative agency pursuant to a subpoena. *See* Cal. Civ. Code §§ 56.10(b)(3) and 56.10(b)(6).

(h) States a specific date after which the provider of health care, health care service plan, pharmaceutical company, or contractor is no longer authorized to disclose the medical information.

(i) Advises the person signing the authorization of the right to receive a copy of the authorization.

Cal. Civ. Code § 56.11.

21. Moreover, a health care provider that maintains information for purposes covered by the CMIA is liable for negligent disclosures that arise as the result of an affirmative act—such as implementing a system that records and discloses online patients personally identifiable information and protected health information. Cal. Civ. Code § 56.36(c).<sup>4</sup> Similarly, if a negligent release occurs and medical information concerning a patient is improperly viewed or otherwise accessed, the individual need not suffer actual damages. Cal. Civ. Code § 56.36(b).

22. “In addition to any other remedies available at law, any individual may bring an action against any person or entity who has negligently released confidential information or records concerning him or her in violation of this part, for either or both of the following: [¶] (1) ... nominal damages of one thousand dollars (\$1,000). In order to recover under this paragraph, it shall not be necessary that the plaintiff suffered or was threatened with actual damages. [¶] (2) The amount of actual damages, if any, sustained by the patient.” *Sutter Health v. Superior Ct.*, 227 Cal. App. 4th 1546, 1551, 174 Cal. Rptr. 3d 653, 656 (2014) (quoting Cal. Civ. Code § 56.36(b)).

### C. Instant Urgent Care’s Website

23. Instant Urgent Care is “a healthcare facility that provides immediate medical help for non-life-threatening conditions.”<sup>5</sup> Instant Urgent Care offers a variety of urgent care medical services, including general illness visits and STD testing.<sup>6</sup> Outside of its urgent care service, Instant Urgent Care also offers a variety of primary care medical services, including flu shots,

<sup>4</sup> “Every provider of health care ... who creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall do so in a manner that preserves the confidentiality of the information contained therein. Any provider of health care ... who negligently creates, maintains, preserves, stores, abandons, destroys, or disposes of medical information shall be subject to the remedies and penalties provided under subdivisions (b) and (c) of Section 56.36.” (§ 56.101, subd. (a).)

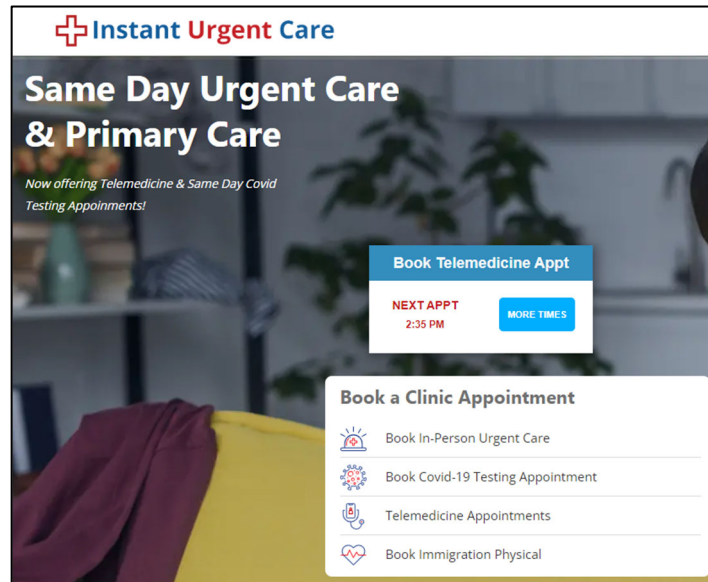
<sup>5</sup> INSTANT URGENT CARE, <https://instantuc.com/about-us/>.

<sup>6</sup> INSTANT URGENT CARE, <https://instantuc.com/urgent-care/>.

cancer screenings, and wellness exams.<sup>7</sup> Patients can book telehealth or in-person appointments through Defendant's Website. Instant Urgent Care has 10 locations in the San Francisco Bay Area region.<sup>8</sup>

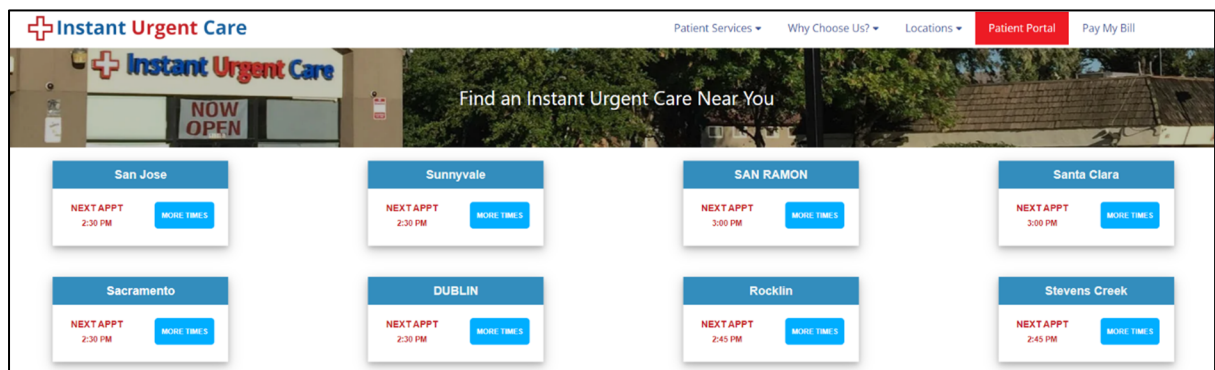
24. When consumers access Instant Urgent Care's Website, they are immediately encouraged to schedule an appointment online, as depicted in Figure 1 below:

**Figure 1**



25. When users proceed to schedule an appointment online they are then directed to select the location of the Instant Urgent Care center they intend on visiting:

**Figure 2**



<sup>7</sup> INSTANT URGENT CARE, <https://instantuc.com/patients-services/>.

<sup>8</sup> INSTANT URGENT CARE, <https://instantuc.com/locations/>.



26. After consumers have selected a location, they are then directed to select the time and type of their appointment:

**Figure 3**

27. However, unbeknownst to consumers, after selecting the location of their appointment they are then redirected off the Instant Urgent Care Website and onto the Online Booking Platform hosted by Practice Crown Inc.

28. Consumers are not alerted that they are leaving the Instant Urgent Care Website and now communicating with an unknown third party. Defendants also fail to provide consumers with privacy policies detailing such practices.

#### **D. Practice Crown Inc.’s Services and Online Booking Platform**

29. Defendant Practice Crown Inc. markets itself as a “strategic partner is managing and growing”<sup>9</sup> private medical practices, like Instant Urgent Care.

30. Defendant Practice Crown Inc. offers many services to its clients, including “cutting-edge website development,” “targeted digital marketing,” and “seamless online appointment booking.”<sup>10</sup>

31. As shown in Figure 3, consumers have no indication that they are now interacting with an unknown third party. That is by design. Defendant Practice Crown Inc. intentionally mimics its client’s webpages to give the illusion that consumers are still communicating directly with their health care provider.

<sup>9</sup> PRACTICE CROWN INC., <https://practicecrown.com/about>.

<sup>10</sup> *Id.*

32. Once consumers select their appointment type and a time for their visit, they are brought to another page to finalize their appointment with Defendant Instant Urgent Care. Unbeknownst to consumers, the webpage in Figures 4 and 5 is hosted by Defendant Practice Crown Inc.:

**Figure 4**

The screenshot shows the Instant Urgent Care website. At the top left is the logo "Instant Urgent Care" with a red cross icon. At the top right is a "LOG IN" button. Below the logo is a purple box containing the location name "Sunnyvale" and its address: "970 W El Camino Real Ste 8 Sunnyvale CA 94087" and phone number: "(408) 212-7420". Below this is a "Patient Information" section with a blue button labeled "Patient Information". Underneath, it shows the appointment time: "When: 06/17/24, 4:30 PM" and the patient type: "Type: sick". At the bottom, a yellow banner states: "We're holding your appointment while you complete your booking - 05:29".

**Figure 5**

The screenshot shows the patient information form on the Instant Urgent Care website. The form includes the following fields: First Name \*, MI, Last Name \*, Email Address \*, Month \*, Day \*, YYYY \*, Legal Sex \*, SSN, Mobile \*, Marital Status \*, Address \*, APT, Zip \*, City \*, State \*, Payment Mode, Reason for Visit \*, Signature \*, and a checkbox for "I have read and accept Terms & Conditions.\*". A blue "Submit" button is located at the bottom right.

33. As shown in Figure 5, consumers are required to fill out several fields requesting sensitive medical and personally identifiable information in order to confirm their medical appointment with Defendant Instant Urgent Care. Such information includes consumers' name, sex, date of birth, home address, email address, marital status, social security number, and the reason for their medical appointment.

34. As shown in Figure 6, all of this protected information is disclosed to Defendant Practice Crown Inc. without consumers' knowledge or consent:

**Figure 6**

```

"Username": "abc",
"PracticeId": 11381,
"DepartmentId": 2,
"AppointmentId": 100292470,
"AppointmentTypeId": "221",
"FirstName": "Sophia",
"MiddleName": "",
"LastName": "Anderson",
"Day": "10",
"Month": "07",
"Year": "2001",
"DOB": "07/10/2001",
"email": "thommy5431@yahoo.com",
"ssn": "639047788",
"Phone": "9542959032",
"address1": "15664 Kalisher St",
"address2": "",
"zip": "91344",
"expirationmonthmm": "11",
"expirationyearyyyy": "2029",
"billingzip": "93131",
"city": "Granada Hills",
"state": "CA",
"maritalstatus": "X",
"guarantorrelationshippatient": 1,
"guarantorfirstname": "Sophia",
"guarantormiddlename": "",
"guarantorlastname": "Anderson",
"CDay": "",
"CMonth": "",
"CYear": "",
"guantordob": "07/10/2001",
"guarantorphone": "9542959032",
"guantoremail": "thommy5431@yahoo.com",
"guantorssn": "639047788",
"guantoraddress1": "15664 Kalisher St",
"guantorcity": "Granada Hills",
"guantorstate": "CA",
"guantorzip": "91344",
"sex": "F",
"insuranceidnumber": "",
"InsuranceMemberId": "",
"IsFirstVisit": "true",
"ReasonforVisit": "Genital warts testing,"

```

35. Defendants then leverage this information, in part, for targeted advertising purposes.

36. Defendant Instant Urgent Care allows Defendant Practice Crown Inc. to receive the confidential PHI and PII of its patients in violation of California law.

#### **E. Facebook's Platform and its Business Tools**

37. In addition to the disclosures described, *supra*, both Defendants host code for the Meta Pixel on the Website and on the Online Booking Platform.

38. Facebook describes itself as a “real identity platform,”<sup>11</sup> meaning users are allowed only one account and must share “the name they go by in everyday life.”<sup>12</sup> To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.<sup>13</sup>

39. In 2021, Facebook generated \$117 billion in revenue.<sup>14</sup> With respect to the apps offered by Facebook, substantially all of Facebook’s revenue is generated by selling advertising space.<sup>15</sup>

40. Facebook sells advertising space by highlighting its ability to target users.<sup>16</sup> Facebook can target users so effectively because it surveils user activity both on and off its site.<sup>17</sup> This allows Facebook to make inferences about users beyond what they explicitly disclose, like their “interests,” “behavior,” and “connections.”<sup>18</sup> Facebook compiles this information into a generalized dataset called “Core Audiences,” which allows advertisers to reach precise audiences based on specified targeting types.<sup>19</sup>

41. Advertisers can also build “Custom Audiences.”<sup>20</sup> Custom Audiences enables advertisers to reach “people who have already shown interest in [their] business, whether they’re

<sup>11</sup> Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).

<sup>12</sup> META TRANSPARENCY CENTER, FACEBOOK COMMUNITY STANDARDS, [https://www.facebook.com/communitystandards/integrity\\_authenticity](https://www.facebook.com/communitystandards/integrity_authenticity).

<sup>13</sup> FACEBOOK, SIGN UP, <https://www.facebook.com/>.

<sup>14</sup> META INVESTOR RELATIONS, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, <https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx>.

<sup>15</sup> *Id.* at 63.

<sup>16</sup> META, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES, <https://www.facebook.com/business/help/205029060038706>.

<sup>17</sup> META, ABOUT META PIXEL, <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

<sup>18</sup> META, AUDIENCE AD TARGETING: HOW TO FIND PEOPLE MOST LIKELY TO RESPOND TO YOUR AD., <https://www.facebook.com/business/ads/ad-targeting>.

<sup>19</sup> META, CORE AUDIENCES, <https://www.facebook.com/business/news/Core-Audiences>.

<sup>20</sup> META, ABOUT CUSTOM AUDIENCES, <https://www.facebook.com/business/help/744354708981227?id=2469097953376494>.

loyal customers or people who have used [their] app or visited [their] website.”<sup>21</sup> With Custom Audiences, advertisers can target existing customers directly, and they can also build a “Lookalike Audiences,” which “leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities.”<sup>22</sup> Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook’s “Business Tools.”<sup>23</sup>

42. As Facebook puts it, the Business Tools “help website owners and publishers, app developers and business partners, including advertisers and others, integrate with [Facebook], understand and measure their products and services, and better reach and serve people who might be interested in their products and services.”<sup>24</sup> Put more succinctly, Facebook’s Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

43. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage’s Universal Resource Locator (“URL”) and metadata, or when a user downloads a mobile application or makes a purchase.<sup>25</sup> Facebook’s Business Tools can also track other events. Facebook offers a menu of “standard events” from which advertisers can

<sup>21</sup> META, AUDIENCE AD TARGETING, <https://www.facebook.com/business/ads/ad-targeting>.

<sup>22</sup> META, ABOUT LOOKALIKE AUDIENCES, <https://www.facebook.com/business/help/164749007013531?id=401668390442328>.

<sup>23</sup> META, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, <https://www.facebook.com/business/help/170456843145568?id=2469097953376494>; META, *Create a website custom audience*, <https://www.facebook.com/business/help/1474662202748341?id=2469097953376494>.

<sup>24</sup> META, THE META BUSINESS TOOLS, <https://www.facebook.com/help/331509497253087>.

<sup>25</sup> See META FOR DEVELOPERS, GUIDES: ADVANCED, <https://developers.facebook.com/docs/facebook-pixel/advanced/>; see also META, BEST PRACTICES FOR META PIXEL SETUP, <https://www.facebook.com/business/help/218844828315224?id=1205376682832142>; META, APP EVENTS API, <https://developers.facebook.com/docs/marketing-api/app-event-api/>.

1 choose, including what content a visitor views or purchases.<sup>26</sup> Advertisers can even create their  
 2 own tracking parameters by building a “custom event.”<sup>27</sup>

3 44. One such Business Tool is the Meta Pixel (the “Meta Pixel”). Facebook offers this  
 4 piece of code to advertisers, like Defendants, to integrate into their websites. The Meta Pixel  
 5 “tracks the people and type of actions they take.”<sup>28</sup> When a user accesses a website hosting the  
 6 Meta Pixel, Facebook’s software script surreptitiously directs the user’s browser to  
 7 contemporaneously send a separate message to Facebook’s servers. This second, secret  
 8 transmission contains the original GET request sent to the host website, along with additional data  
 9 that the Meta Pixel is configured to collect. This transmission is initiated by Facebook code and  
 10 concurrent with the communications with the host website. At relevant times, two sets of code are  
 11 thus automatically run as part of the browser’s attempt to load and read Defendant Instant Urgent  
 12 Care’s Website and Defendant Practice Crown Inc.’s Online Booking Platform—Defendants’ own  
 13 code, and Facebook’s embedded code.

14 45. Defendants chose to include the Meta Pixel on both the Website and the Online  
 15 Booking Platform.

16 46. Facebook’s own documentation makes clear just how much tracking of private  
 17 information the Meta Pixel does. It describes the Meta Pixel as code that Facebook’s business  
 18 customers can put on their website to “[m]ake sure your ads are shown to the right people. *Find ...*  
 19 *people who have visited a specific page or taken a desired action on your website.*” (Emphasis  
 20 added.)<sup>29</sup>

21 47. Facebook instructs such business customers that:

22 Once you’ve set up the [Facebook Tracking] Pixel, *the pixel will log when someone takes*

23 <sup>26</sup> META, SPECIFICATIONS FOR META PIXEL STANDARD EVENTS,  
 24 <https://www.facebook.com/business/help/402791146561655?id=1205376682832142>.

25 <sup>27</sup> META, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,  
 26 <https://www.facebook.com/business/help/964258670337005?id=1205376682832142>; *see also*  
 27 META FOR DEVELOPERS, APP EVENTS API, [https://developers.facebook.com/docs/marketing-](https://developers.facebook.com/docs/marketing-api/app-event-api/)  
 28 [api/app-event-api/](https://developers.facebook.com/docs/marketing-api/app-event-api/).

<sup>28</sup> META, RETARGETING, <https://www.facebook.com/business/goals/retargeting>.

<sup>29</sup> META, ABOUT META PIXEL,  
<https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

1 *an action on your website.* Examples of actions include adding an item to their shopping  
 2 cart or making a purchase. *The Pixel receives these actions, or events*, which you can view  
 3 on your [Facebook Tracking] Pixel page in Events Manager. From there, you'll be able to  
 4 see the actions that your customers take. *You'll also have options to reach those customers  
 again through future Meta ads.*<sup>30</sup>

48. Of course, in healthcare, it is medical specialists that users “add to their shopping  
 5 cart.” Patients make doctor’s appointments rather than making purchases.

49. The Meta Pixel code enables Facebook not only to help Defendants with advertising  
 7 to its own patients outside the Website, but also to include individual patients among groups  
 8 targeted by *other* Facebook advertisers relating to the conditions about which patients  
 9 communicated on the Website.

50. Facebook’s Business Help Center explains:

Meta *uses marketing data to show ads to people who are likely to be interested in them.*  
 12 One type of marketing data is website events, which are *actions that people take on your  
 website.*<sup>31</sup>

51. In other words, Facebook sells advertising space by highlighting its ability to target  
 14 users.<sup>32</sup> Facebook can target users so effectively because it surveils user activity both on and off its  
 15 site.<sup>33</sup> This allows Facebook to make inferences about users beyond what they explicitly disclose,  
 16 like their “interests,” “behavior,” and connections.<sup>34</sup>

52. An example illustrates how the Meta Pixel works. Take an individual who  
 18 navigates to the Website and clicks on the link for “Book In-Person Urgent Care” on the  
 19 homepage. When that “Book In-Person Urgent Care” link is clicked, the individual’s browser  
 20 sends a GET request to Defendant’s server requesting that server to load the particular webpage.  
 21 Because Defendant Instant Urgent Care and Defendant Practice Crown Inc. utilize the Meta Pixel,

22 <sup>30</sup> *Id.* (Emphasis added.)

23 <sup>31</sup> META, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS,  
 24 <https://www.facebook.com/business/help/964258670337005?id=1205376682832142> (emphasis  
 added).

25 <sup>32</sup> META, WHY ADVERTISE ON FACEBOOK, INSTAGRAM AND OTHER META TECHNOLOGIES,  
 26 <https://www.facebook.com/business/help/205029060038706> (last visited Dec. 26, 2023).

27 <sup>33</sup> META, ABOUT META PIXEL,  
 28 <https://www.facebook.com/business/help/742478679120153?id=1205376682832142>.

<sup>34</sup> META, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS,  
<https://www.facebook.com/business/ads/ad-targeting>.

Facebook’s embedded code, written in JavaScript, sends secret instructions back to the individual’s browser, without alerting the individual that this is happening. Facebook causes the browser to secretly duplicate the communication with Defendants, transmitting it to Facebook’s servers, alongside additional information that transcribes the communication’s content and the individual’s identity.

53. After collecting and intercepting the information described in the preceding paragraph, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

**F. Defendant Instant Urgent Care Disclosed Plaintiff’s and Class Members’ Protected Health Information to Practice Crown Inc. and Facebook and Assisted Facebook with Intercepting Communications**

54. Defendant Instant Urgent Care assists Defendant Practice Crown Inc. and Facebook in obtaining its patients’ protected health information (“PHI”) and personally identifiable information (“PII”) when they schedule appointments on the Website through the Online Booking Platform.

55. Through the Meta Pixel, Defendants assisted Facebook in intercepting the identities and online activity of Defendant Instant Urgent Care’s patients, including information related to the type of medical treatment patients were seeking and the location.

56. When a patient enters <https://instantuc.com/>, they are able to book a clinic appointment. *See* Figure 1, *supra*.

57. By clicking on the “Book In-Person Urgent Care” link, a patient is directed to a page on Defendant’s website where they can see available appointments and locations. *See* Figure 2, *supra*.

58. After a patient selects a location and time for their appointment, they are directed to the “Patient Information” page. *See* Figure 5, *supra*.

59. Due to the integration of the Meta Pixel on the Website, Facebook is able to intercept the information about the Website page the patient reached. This information includes the location of the appointment, which is included in the “dl” and “rl” values:



**Figure 7**

```

id 234615969492023
ev PageView
dl https://practicecrown.com/d/appointment/book-appointment?data=[{"queryParams":{"at_id":101,"a_id":100203597,"starttime":"9:30 AM","app_date":"04/17/2024","app_type":"Sick Visit","providername":"Scheduling
Provider_RK","did":"25","pid":"11381","Udc":"Ro85204"}}]
rl https://instantuc.com/

```

60. As shown in Figure 7, the Meta Pixel intercepts information contained in the URL values for the webpages visited by patients of Defendant Instant Urgent Care, including “book-appointment,” “starttime: 9:30AM,” app\_date: 04/17/2024,” “app\_type: Sick Visit,” and “Scheduling Provider\_RK.”

61. The data listed in the “rl” value intercepted by the Meta Pixel allows Facebook to know that this information relates to consumers’ use of the “instantuc.com” Website, the Website for Defendant Instant Urgent Care.

62. When Facebook intercepts this communication due to Defendants’ integration of the Meta Pixel on both the Website and the Online Booking Platform, Facebook is informed of the creation of the urgent care appointment, the reason for the appointment, and the location and time of the appointment.

63. Each time Facebook intercepts this activity data via the Meta Pixel integrated into the Website and the Online Booking Platform by Defendants, it also intercepts a patient’s personally identifiable information, including their Facebook ID (“FID”). A FID is a unique and persistent identifier that Facebook assigns to each user. With it, anyone ordinary person can look up the user’s Facebook profile and name. Notably, while Facebook can easily identify any individual on its Facebook platform with only their unique FID, so too can any ordinary person who comes into possession of an FID. Facebook admits as much on its website. Indeed, ordinary persons who come into possession of the FID can connect to any Facebook profile.

64. A user who accesses the Website and Online Booking Platform while logged into Facebook will transmit the c\_user cookie to Facebook, which contains that user’s unencrypted Facebook ID.

65. When a visitor’s browser has recently logged out of an account, Facebook compels the visitor’s browser to send a smaller set of cookies.

66. One such cookie is the “fr cookie” which contains, at least, an encrypted Facebook ID and browser identifier.<sup>35</sup> Facebook, at a minimum, uses the fr cookie to identify users.<sup>36</sup>

67. If a visitor has never created an account, an even smaller set of cookies are transmitted.

68. At each stage, Defendants also utilizes the “\_fbp cookie”, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a user.<sup>37</sup>

69. The c\_user cookie expires after 90 days if the user checked the “keep me logged in” checkbox on the website.<sup>38</sup> Otherwise, the c\_user cookie is cleared when the browser exits.<sup>39</sup>

70. The fr cookie expires after 90 days unless the visitor’s browser logs back into Facebook.<sup>40</sup> If that happens, the time resets, and another 90 days begins to accrue.<sup>41</sup>

71. The \_fbp cookie expires after 90 days unless the visitor’s browser accesses the same website.<sup>42</sup> If that happens, the time resets, and another 90 days begins to accrue.<sup>43</sup>

72. The Meta Pixel uses both first- and third-party cookies. A first-party cookie is “created by the website the user is visiting”—*i.e.*, Instant Urgent Care.<sup>44</sup> A third-party cookie is “created by a website with a domain name other than the one the user is currently visiting”—*i.e.*,

<sup>35</sup> DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21, 2012), [http://www.europe-v-facebook.org/ODPC\\_Review.pdf](http://www.europe-v-facebook.org/ODPC_Review.pdf).

<sup>36</sup> META, PRIVACY CENTER—COOKIES POLICY, <https://www.facebook.com/privacy/policies/cookies/?subpage=subpage-1.3>.

<sup>37</sup> META, COOKIES & OTHER STORAGE TECHNOLOGIES, <https://www.facebook.com/policy/cookies/>.

<sup>38</sup> Seralthan, FACEBOOK COOKIES ANALYSIS (Mar. 14, 2019), <https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbf8a>.

<sup>39</sup> *Id.*

<sup>40</sup> *See id.*

<sup>41</sup> Confirmable through developer tools.

<sup>42</sup> *See* META, COOKIES & OTHER STORAGE TECHNOLOGIES, <https://www.facebook.com/policy/cookies/>.

<sup>43</sup> Also confirmable through developer tools.

<sup>44</sup> PC MAG, FIRST-PARTY COOKIES, <https://www.pcmag.com/encyclopedia/term/first-party-cookie>. This is confirmable by using developer tools to inspect a website’s cookies and track network activity.

Facebook.<sup>45</sup> The \_fbp cookie is always transmitted as a first-party cookie. A duplicate \_fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

73. Facebook, at a minimum, uses the fr, \_fbp, and c\_user cookies to link to Facebook IDs and corresponding Facebook profiles. Defendants sent these identifiers alongside the event data.

74. Plaintiff used the Website and Online Booking Platform to book an urgent care appointment. Plaintiff never consented, agreed, authorized, or otherwise permitted Defendant Practice Crown Inc. to access his highly sensitive and confidential PHI and PII. Similarly, Plaintiff never consented, agreed, authorized, or otherwise permitted Defendants to disclose his PII and PHI to Facebook via the Meta Pixel. Plaintiff was never provided with any written notice that Defendants integrated code into the Website and Online Booking Platform that allowed Facebook to intercept Website users' PHI and PII, nor was he provided any means of opting out of such disclosures.

75. In fact, Defendants failed to provide any privacy policy to Plaintiff and putative class members' about how their sensitive and protected data would be protected.

76. By law, Plaintiff is entitled to privacy in his PHI and confidential communications. Defendants deprived Plaintiff of his privacy rights when it: (1) implemented a system that surreptitiously allowed Facebook, to track, record, and intercept Plaintiff's and other online patients' confidential communications, PII, and PHI; and (2) undertook this pattern of conduct without notifying Plaintiff and without obtaining his express written consent.

### **CLASS ALLEGATIONS**

77. Class Definition: Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of himself and other similarly situated individuals defined as all persons in the United States who, during the class period, scheduled an online appointment for medical treatment on a platform hosted by Practice Crown Inc. (the "Class").

<sup>45</sup> PC MAG, THIRD-PARTY COOKIE, <https://www.pcmag.com/encyclopedia/term/third-party-cookie>. This is also confirmable by tracking network activity.

1           78. Plaintiff also seeks to represent a subclass consisting of Class members who, during  
2 the class period, maintained an active Facebook account and scheduled an appointment on the  
3 Website and Online Booking Platform while located in California (the “Subclass”).

4           79. Plaintiff reserves the right to modify the class definition or add sub-classes as  
5 necessary prior to filing a motion for class certification.

6           80. The “Class Period” is the time period beginning on the date established by the  
7 Court’s determination of any applicable statute of limitations, after considering of any tolling,  
8 concealment, and accrual issues, and ending on the date of entry of judgement.

9           81. Excluded from the Class and Subclass is Instant Urgent Care; any affiliate, parent,  
10 or subsidiary of Instant Urgent Care; any entity in which Instant Urgent Care has a controlling  
11 interest; any officer director, or employee of Instant Urgent Care; any successor or assign of Instant  
12 Urgent Care;; Practice Crown Inc.; any affiliate, parent, or subsidiary of Practice Crown Inc.; any  
13 entity in which Practice Crown Inc. has a controlling interest; any officer director, or employee of  
14 Practice Crown Inc.; any successor or assign of Practice Crown Inc.; anyone employed by counsel  
15 in this action; any judge to whom this case is assigned, his or her spouse and immediate family  
16 members; and members of the judge’s staff.

17           82. Numerosity/Ascertainability. Members of the Class and Subclass are so numerous  
18 that joinder of all members would be unfeasible and not practicable. The exact number of Class  
19 and Subclass Members is unknown to Plaintiff at this time; however, it is estimated that there are  
20 hundreds of thousands of individuals in the Class and Subclass. The identity of such membership  
21 is readily ascertainable from Defendants’ records and non-party records, such as those of  
22 Facebook.

23           83. Typicality. Plaintiff’s claims are typical of the claims of the Class and Subclass  
24 because Plaintiff used the Website and, as a result of Defendants’ unlawful conduct, had his PII  
25 and PHI disclosed to Defendant Practice Crown Inc. and intercepted by Facebook, without his  
26 express written authorization or knowledge. Plaintiff’s claims are based on the same legal theories  
27 as the claims of other Class and Subclass Members.  
28

84. Adequacy. Plaintiff is fully prepared to take all necessary steps to represent fairly and adequately the interests of the Class and Subclass Members. Plaintiff's interests are coincident with, and not antagonistic to, those of the members of the Class and Subclass. Plaintiff is represented by attorneys with experience in the prosecution of class action litigation generally and in the emerging field of digital privacy litigation specifically. Plaintiff's attorneys are committed to vigorously prosecuting this action on behalf of the members of the Class and Subclass.

85. Common Questions of Law and Fact Predominate/Well Defined Community of Interest. Questions of law and fact common to the members of the Class and Subclass predominate over questions that may affect only individual members of the Class and Subclass because Defendants have acted on grounds generally applicable to the Class and Subclass. Such generally applicable conduct is inherent in Defendants' wrongful conduct. Questions of law and fact common to the Classes include:

- a. Whether Defendants intentionally tapped the lines of internet communication between patients and their medical providers;
- b. Whether Instant Urgent Care's Website contains code that permits third parties, such as Facebook, to intercept patients' personally identifiable information, protected health information, and related communications;
- c. Whether Practice Crown Inc.'s Online Booking Platform contains code that permits third parties, such as Facebook, to intercept patients' personally identifiable information, protected health information, and related communications;
- d. Whether Facebook is a third-party eavesdropper;
- e. Whether Plaintiff's and Class Members' communications via the Website and the resultant interceptions thereof constitute an affirmative act of communication;
- f. Whether Defendants' conduct, which allowed Facebook—an unauthorized person—to view Plaintiff's and Class Members' personally identifiable information and PHI, resulted in a breach of confidentiality;
- g. Whether Instant Urgent Care violated Plaintiff's, Class, and Subclass Members' privacy rights by using third-party technology, such as the Online Booking Platform

and Meta Pixel, to allow third parties to access and/or intercept patients' online communications along with information that uniquely identified the patients;

- h. Whether Plaintiff, Class, and Subclass Members are entitled to damages under CIPA, the CMIA, or any other relevant statute; and
- i. Whether Defendants' actions violate Plaintiff's, Class, and Subclass Members' privacy rights as provided by the California Constitution

86. Superiority. Class action treatment is a superior method for the fair and efficient adjudication of the controversy. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, or expense that numerous individual actions would engender. The benefits of proceeding through the class mechanism, including providing injured persons or entities a method for obtaining redress on claims that could not practicably be pursued individually, substantially outweighs potential difficulties in management of this class action. Plaintiff knows of no special difficulty to be encountered in litigating this action that would preclude its maintenance as a class action.

## **CLAIMS FOR RELIEF**

### **COUNT I**

#### **Violation Of The California Invasion Of Privacy Act, Cal. Penal Code § 631 (On Behalf Of The Class and Subclass)**

87. Plaintiff repeats the allegations contained in the paragraphs above as if fully set forth herein and brings this count individually and on behalf of the members of the Class and Subclass.

88. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. CIPA begins with its statement of purpose—namely, that the purpose of CIPA is to "protect the right of privacy of the people of [California]" from the threat posed by "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications ... " Cal. Penal Code § 630.

89. A person violates California Penal Code § 631(a), if:

by means of any machine, instrument, or contrivance, or in any other manner, [s/he] intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or [s/he] willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or [s/he] uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained ...

Cal. Penal Code § 631(a).

90. Further, a person violates § 631(a) if s/he “aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned” in the preceding paragraph. *Id.*

91. To avoid liability under § 631(a), a defendant must show it had the consent of all parties to a communication.

92. At all relevant times, Defendants aided, agreed with, and conspired with Facebook to track and intercept Plaintiff’s and Class Members’ internet communications while accessing the Website and Online Booking Platform. These communications were intercepted without the authorization and consent of Plaintiff and Class Members.

93. Defendants, when aiding and assisting the wiretapping by Facebook, intended to help Facebook learn some meaning of the content in the URLs and the content the visitor requested.

94. The following items constitute “machine[s], instrument[s], or contrivance[s]” under the CIPA, and even if they do not, the Meta Pixel falls under the broad catch-all category of “any other manner”:

- a. The computer codes and programs Facebook used to track Plaintiff and Class Members’ communications while they were navigating the Website and Online Booking Platform;
- b. Plaintiff’s and Class Members’ browsers;

- c. Plaintiff's and Class Members' computing and mobile devices;
- d. Facebook's web and ad servers;
- e. The web and ad-servers from which Facebook tracked and intercepted the Plaintiff's and Class Members' communications while they were using a web browser to access or navigate the Website and Online Booking Platform;
- f. The computer codes and programs used by Facebook to effectuate its tracking and interception of the Plaintiff's and Class Members' communications while they were using a browser to visit the Website and the Online Booking Platform; and
- g. The plan Facebook carried out to effectuate their tracking and interception of the Plaintiff's and Class Members' communications while they were using a web browser to visit the Website and Online Booking Platform.

95. The patient communication information that Defendants permitted Facebook to intercept via their integration of the Meta Pixel, including doctor appointment booking information and the reason, time, and location of the appointment constitutes PHI.

96. As demonstrated hereinabove, Defendants violated CIPA by aiding and permitting third parties like Facebook to receive its patients' online communications through the Website and Online Booking Platform without their consent.

97. As a result of the above violations, Defendants are liable to Plaintiff and other Subclass Members in the amount of, the greater of, \$5,000 dollars per violation or three times the amount of actual damages. Additionally, Cal. Penal Code § 637.2 specifically states that "[it] is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages."

98. Under the statute, Defendants are also liable for reasonable attorney's fees, and other litigation costs, injunctive and declaratory relief, and punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by the Defendants in the future.



**COUNT II****Violation of the California Confidentiality of Medical Information Act  
Cal. Civ. Code § 56.10  
(On Behalf Of The Class and Subclass)**

99. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class and Subclass.

100. Under the California Confidentiality of Medical Information Act, Cal. Civ. Code § 56.10 (“CMIA”), providers of health care are prohibited from disclosing medical information relating to their patients, without a patient’s authorization. Medical information refers to “any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care ... regarding a patient's medical history, mental or physical condition, or treatment. “Individually Identifiable” means that the medical information includes or contains any element of personal identifying information sufficient to allow identification of the individual...”

101. The CMIA § 56.06(a) defines a provider of health care as “[a]ny business organized for the purpose of maintaining medical information in order to make the information available to an individual or to a provider of health care at the request of the individual or a provider of health care, for purposes of allowing the individual to manage the individual's information, or for the diagnosis and treatment of the individual”

102. Plaintiff and Class Members are patients under the definition of the CMIA because Plaintiff and Class Members received “health care services from a provider of health care” and the information Defendant Instant Urgent Care disclosed to Defendant Practice Crown Inc. was “medical information pertain[ing]” to Plaintiff and Class Members. Cal. Civ. Code § 56.05(m).

103. Defendant Instant Urgent Care is a provider of health care under Cal. Civ. Code § 56.06(a) because it is an organization designed to provide patients with access to health care and provides a platform from which patients can manage their diagnosis or treatment of their medical conditions. Because Defendant Instant Urgent Care is deemed a provider of health care, it has an ongoing obligation to comply with the CMIA’s requirements regarding the maintenance of its user’s medical information.

104. As set forth hereinabove, Defendant Instant Urgent Care disclosed to Defendant Practice Crown Inc. several pieces of information regarding its patients' use of its Website, which, included, but is not limited to: name, sex, date of birth, home address, email address, marital status, social security number, and the reason for their medical appointment.

105. This patient information is derived from a provider of health care regarding patients' medical treatment and physical condition. Accordingly, it constitutes medical information pursuant to the CMIA.

106. Defendant Instant Urgent Care fails to protect its patients protected health information and personally identifiable information as required by HIPAA. Defendant Instant Urgent Care also fails to provide its patients with a privacy policy detailing how it would protect such information.

107. As demonstrated hereinabove, Defendant Instant Urgent Care failed to maintain the privacy and security of its patients' protected health information. Based on the above, Defendant Instant Urgent Care violated the CMIA by disclosing its patients' medical information to Defendant Practice Crown Inc. while failing to obtain patient's valid authorization for the disclosure of their medical information.

108. Under the CMIA, a patient may recover compensatory damages, punitive damages not to exceed \$3,000 dollars and attorneys' fees not to exceed \$1,000, and the costs of litigation for any violating disclosure of medical information. Alternatively, a patient may recover nominal damages of \$1,000 for any negligent release of medical information.

**COUNT III**  
**Violation of the California Invasion of Privacy Act**  
**Cal. Penal Code § 632**

109. Plaintiffs incorporate the preceding paragraphs as if fully set forth herein.

110. Plaintiff Tim Harvey brings this claim against Defendant Practice Crown Inc. individually and on behalf of the Class.

111. CIPA § 632(a) prohibits an entity from:

intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to

1 eavesdrop upon or record the confidential communication, whether the  
2 communication is carried on among the parties in the presence of one  
3 another or by means of a telegraph, telephone, or other device, except a  
radio.

4 112. Practice Crown Inc. software is an “electronic amplifying or recording device[s].”

5 113. The following pieces of information provided by Plaintiff Tim Harvey and  
6 California Class Members to Practice Crown Inc. constitute “confidential communications”:  
7 Plaintiff’s medical symptoms, name, sex, date of birth, home address, email address, marital status,  
8 and social security number.

9 114. At all relevant times, Defendant Practice Crown Inc. intentionally eavesdropped on  
10 the confidential communications of Plaintiff Tim Harvey and Class Members.

11 115. When communicating with the Website, Plaintiff Harvey and Class Members had an  
12 objectively reasonable expectation of privacy. Plaintiff Harvey and Class Members did not  
13 reasonably expect that anyone other than Instant Urgent Care would be on the other end of the  
14 communication, and that other, third-party entities like Practice Crown Inc. would intentionally use  
15 an electronic amplifying or recording device to eavesdrop upon and record the confidential  
16 communications of Plaintiff and Class Members. Indeed, Plaintiff and Class Members each  
17 communicated Personally Identifying Information (PII) and Protected Health Information (PHI) to  
18 the Website as alleged above, which enhanced their reasonable expectation of privacy because such  
19 secretive communications should not be disclosed to or intercepted by third parties like Defendant  
20 Practice Crown Inc.

21 116. Plaintiff Harvey and Class Members did not consent to any of Practice Crown’s  
22 actions. Nor have Plaintiff or Class Members consented to Practice Crown’s intentional use of an  
23 electronic amplifying or recording device to eavesdrop upon and record the confidential  
24 communications of Plaintiff and Class Members.

25 117. Pursuant to Cal. Penal Code § 637.2, Plaintiff Harvey and California Class  
26 Members have been injured by Practice Crown Inc.’s violations of CIPA § 632(a), and each seeks  
27 statutory damages of \$5,000 for each of Practice Crown Inc.’s violations of CIPA § 632(a).  
28

**COUNT IV**  
**Invasion Privacy Under California's Constitution**  
**(On Behalf Of The Class and Subclass)**

118. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set forth herein and brings this claim individually and on behalf of the proposed Class and Subclass.

119. Plaintiff, Class, and Subclass Members have an interested in: (1) precluding the dissemination and/or misuse of their sensitive, confidential communications and protected health information; and (2) making personal decisions and/or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various internet sites without being subjected to wiretaps without Plaintiff, Class, and Subclass Members' knowledge or consent.

120. At all relevant times, by unlawfully disclosing patients' medical information and personally identifiable information, Defendants intentionally invaded Plaintiff's, Class Members' privacy rights under the California Constitution.

121. Similarly, at all relevant times, by using the Meta Pixel to record and communicate patients' FIDs, IP addresses, and device identifiers alongside their confidential medical communications, Defendants intentionally invaded Plaintiff's and Subclass Members' privacy rights under the California Constitution.

122. Plaintiff, Class, and Subclass Members had a reasonable expectation that their communications, identity, health information and other data would remain confidential and that Instant Urgent Care would not disclose such information to unknown third parties and that Defendants would not install wiretaps on the Website and the Online Booking Platform.

123. Plaintiff, Class, and Subclass Members did not authorize Defendants to record and transmit Plaintiff's, Class, and Subclass Members' private medical communications alongside their personally identifiable health information.

124. This invasion of privacy is serious in nature, scope, and impact because it relates to patients' private medical communications. Moreover, it constituted an egregious breach of the societal norms underlying the privacy right.

125. Accordingly, Plaintiff, Class, and Subclass Members seek all relief available for invasion of privacy claims under California's Constitution.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for relief and judgment, as follows:

- a. For a determination that this action is a proper class action;
- b. For an order certifying the Class and Subclass, naming Plaintiff as representative of the Class and Subclass, and naming Plaintiff's attorneys as Class Counsel to represent the Class and Subclass;
- c. For an order declaring that Defendants' conduct violates the statutes referenced herein;
- d. For an order finding in favor of Plaintiff, the Class, and the Subclass on all counts asserted herein;
- e. For an award of compensatory damages, including statutory damages where available, to Plaintiff, Class, and Subclass Members against Defendants for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial;
- f. For punitive damages, as warranted, in an amount to be determined at trial;
- g. For an order requiring Defendants to disgorge revenues and profits wrongfully obtained;
- h. For prejudgment interest on all amounts awarded;
- i. For injunctive relief as pleaded or as the Court may deem proper;
- j. For an order awarding Plaintiff, the Class, and the Subclass their reasonable attorneys' fees and expenses and costs of suit; and
- k. For an order granting Plaintiff, Class, and Subclass Members such further relief as the Court deems appropriate.

**JURY TRIAL DEMANDED**

Plaintiff demands a trial by jury on all claims so triable.

1 Dated: June 27, 2024

**BURSOR & FISHER, P.A.**

2 By: /s/ Brittany S. Scott  
Brittany S. Scott

3  
4 Brittany S. Scott (State Bar No. 327132)  
1990 North California Blvd., Suite 940  
Walnut Creek, CA 94596  
5 Telephone: (925) 300-4455  
6 Facsimile: (925) 407-2700  
E-mail: bscott@bursor.com

7 **BURSOR & FISHER, P.A.**

8 Philip L. Fraietta (State Bar No. 354768)  
1330 Avenue of the Americas, 32nd Floor  
New York, NY 10019  
9 Telephone: (646)-837-7150  
10 Facsimile: (212) 989-9163  
Email: pfraietta@bursor.com

11 *Attorneys for Plaintiff*